	Georgia Technology Authority	
Title:	**Business Continuity and Disaster Recovery**	
PSG Number:	PS-08-025.01	**Topical Area:** Security
Document Type:	Policy	**Pages:** 2
Issue Date:	3/20/08	**Effective Date:** 3/20/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Requires agencies to develop a plan to maintain continuity (recovery and restoration) of essential state government operations and services during or following an emergency.	

PURPOSE

IT resources are essential to an organization's success. Therefore, it is critical that the services provided by these systems are able to operate effectively without excessive interruption while maintaining their required security levels. Contingency planning directly supports an organization's goal of continued operations and is essential to mitigating the risks of system and service unavailability, and financial, legal and regulatory exposure.

This policy requires each agency to have a plan to maintain or recover/restore critical operations in the event of an emergency or disaster.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

POLICY

Agency heads shall create and implement a management structure for business continuity within the agency and for directing the development and execution of a viable disaster recovery and business continuity program.

Agencies shall identify the potential risks that may adversely impact their critical business functions as a result of a natural, man-made, or environmental emergency or disaster, and develop continuity and recovery strategies, plans and procedures that sustain or resume communications and IT functions that support critical business operations and essential constituent services within a specified period of time.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Contingency Planning (Standard)
- Disaster Recovery – System Backups (Standard)

REFERENCES

NIST SP 800-12 (chapter 11) Introduction to Computer Security NIST Handbook
NIST SP 800-34 Contingency Planning Guide

TERMS and DEFINITIONS

Business Continuity Management – The act of anticipating incidents which will affect critical functions and processes for the organization and ensuring that it responds to any incident in a planned and rehearsed manner.

Contingency Plan - Management policy and procedures designed to maintain or restore business operations, including computer operations, in the event of emergencies, system failures, or disaster. Below are other terms often used interchangeably but actually refer to a suite of plans developed to prepare for and execute contingency efforts:

- **IT contingency planning:** The dynamic development of a coordinated recovery strategy for IT systems (major application or general support system), operations, and data after a disruption.
- **Business Continuity Plan (BCP)**: The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.
- **Disaster Recovery Plan (DRP)**: A written plan that details how an organization's applications and/or infrastructure will be recovered or rebuilt and returned to normal operations after a major hardware or software failure or destruction of facilities.
- **Continuity of Operations Plan (COOP)**: A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

Note: PSG number administratively changed from P-08-025.01 on September 1, 2008.